Below are several e-news items that may be of interest, such as the National Governors Association HIPAA Report, information on certification testing and recaps of recent HIPAA news items.

As always: Please be sure to note that in some cases the information presented may be the opinion of the original author. We need to be sure to view it in the context of our own organizations and environment. You may need additional information, support, legal opinions and/or decision documentation when interpreting the rules.

My thanks to all the folks who have shared information for this e-news.
Have a great day!!!
Ken

Interesting items below:

National Governors Association HIPAA Report
[hipaalive] TCS Certification testing
[hipaalive] SECURITY Rule Certification testing
[hipaalive] TCS - Banking
[hipaanotes] HIPAAnote - Vol. 2, No. 23 - 6/19/02 - ATTACHED
[hipaalert] HIPAAlert - Vol. 3, No. 6 - 6/17/02
HIPAA Implementation Newsletter -- Issue #36 - June 14, 2002 - ATTACHED
[hipaanotes] HIPAAnote - Vol. 2, No. 22 - 6/12/02 - ATTACHED
[hipaalert] HIPAAlert-lite - 6/10/02 - ATTACHED

********** National Governers Association HIPAA Report **********
>>> SFrank1@CMS.HHS.GOV 05/30/02 11:43AM >>>
Dear NMEH members,
For a global view, I found the report referenced in the attached quite interesting.
"HIPAA & the States: Critical Issues and Compliance Strategies." It is at:

http://www.nga.org/center/divisions/1,1188,C_ISSUE_BRIEF^D_2717,00.html

Sheila

Sheila Lynn Frank
SFrank1@cms.hhs.gov
CMS / Center for Medicaid & State Operations
Finance, Systems, Quality Group / Division of State Systems
Phone: 410 786-0442

********** [hipaalive] TCS Certification testing **********.
*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***

The CMS web cast last week, informed the viewer that CMS would require Medicare contractors to undergo certification testing. It was also stated that providers should contact their "respective contractor" in order to obtain timeframes for submitter testing. I looked on the HCFA website, but can't find any reference to certification testing requirements. Can anyone point me in the right direction?

Annette Stephens
**** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
Certification is not required by HIPAA, but is recommended by some major industry work groups as a means of validating your system(s) can format, send and receive compliant transactions. I'd recommend you go to the WEDI SNIP site - Work Products at http://snip.wedi.org/public/articles/index.cfm?cat=6 Select the transactions white papers, there is a white paper on testing and certification. You can also search the HIPAAlive archive for messages from Kepa Zubeldia on transaction testing.

Christine Jensen
HIPAA Project Manager

*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
That's correct, CMS isn't requiring providers to certify. But there is potential that the trading partner (payer) may require certification as part of the TPA.

Christine Jensen
HIPAA Project Manager

********** [hipaalive] SECURITY RULE: Certification testing **********.
*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
That is security certification - we were discussing transaction testing and certification.

Christine Jensen
HIPAA Project Manager
Denver Health
303-436-7942

-----Original Message-----
From: Mic Sager [SMTP:MSager@olympicmedical.org]
Sent: Thursday, June 27, 2002 2:40 PM
*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***

Christine - This is cut and paste from the proposed security rule, it seems to require certification.

a. Certification
Each organization would be required to evaluate its computer system(s) or network design(s) to certify that the appropriate security has been implemented. This evaluation could be performed internally or by an external accrediting agency.

We are, at this time, soliciting input on appropriate mechanisms to permit independent assessment of compliance. We would be particularly interested in
input from those engaging in health care electronic data interchange (EDI), as well as independent certification and auditing organizations addressing issues of documentary evidence of steps taken for compliance; need for, or desirability of, independent verification, validation, and testing of system changes; and certifications required for off-the-shelf products used to meet the requirements of this regulation.

We also solicit comments on the extent to which obtaining external certification would create an undue burden on small or rural providers.
- Mic

********** [hipaalive] TCS - Banking **********
*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
The Banking Industry HIPAA Task Force, a joint venture between National Automated Clearing House Association (NACHA) and the American Bankers Association (ABA), has released a white paper to help financial executives understand the banking issues raised by the HIPAA. The white paper includes specific definitions and test cases.
www.nacha.org <http://www.nacha.org/>

Regards,
David Frenkel
Business Development

********** [hipaalert] HIPAAlert - Vol. 3, No. 6 - 6/17/02 **********
>>> <info@phoenixhealth.com> 06/17/02 08:56AM >>>
==========

H I P A A L E R T -- Volume 3, Number 6 -- June 17, 2002

>>From Phoenix Health Systems--HIPAA Knowledge--HIPAA Solutions<<

=> Healthcare IT Consulting & Outsourcing <=

==========
HIPAAlert is published monthly in support of the healthcare industry's efforts to work together towards HIPAA security and privacy. Direct subscribers total over 17,000.

IF YOU LIKE HIPAAlert, YOU'LL LOVE www.HIPAAdvisory.com! -- Phoenix' "HIPAA Hub of the Web"
==========

HAVE YOU INVESTIGATED our new GUIDE TO MEDICAL PRIVACY AND HIPAA -- a comprehensive, 500-page reference on HIPAA how-to's across every compliance phase, including user-friendly analysis and advice by legal and consulting experts, plus sample forms, checklists, workplans and more -- even regular monthly updates and additions for a year!
Learn more: http://www.hipaadvisory.com/wares/HIPAAbook.htm?t

==========

T H I S I S S U E

==========

1 >> F R O M T H E E D I T O R S:

** New Regs Published -- but Security Still Needed **

As promised -- and on schedule! -- the Department of Health and Human Services has delivered its final HIPAA regulation defining a standard Employer Identifier (the Internal Revenue Services's EIN, which businesses that pay employee wages already use), and two new NPRMs amending the Transactions and Code Sets rules. Regarding the regulations' details -- no

real surprises. The effective date of the final Employer Identifier rule is July 30, 2002, with compliance required 24 months later on July 30, 2004. While each of the NPRMs provides for a 30-day comment period from the publication date (May 31), these non-controversial actions should be finalized pretty much as-is, and presumably soon.

From all appearances, more regs are on the way, per the following federal projections:

* Security Final Rule - August 2002
* Claims Attachments NPRM - August 2002
* Health Plan Identifier NPRM - August 2002

Security, of course, is the big one. While organizations across the healthcare industry have become increasingly sensitized to security since 9-11, questions concerning when, what, how, and at what cost security solutions should be implemented have remained unanswered for many, as we await HHS' final security directives. The result is that action across the industry has been slow and sporadic -- perhaps dangerously so. Hopefully, HHS will remain on-track with its mandates for security measures, so that all healthcare organizations -- one, will have no doubts as to what is required of them -- and two, will be further convinced that they have very real vulnerabilities that must be eliminated.

D'Arcy Guerin Gue, Publisher
dgue@phoenixhealth.com

Bruce Hall, Director of Internet Services
bhall@phoenixhealth.com

==========

2 >> H I P A A n e w s

** Cybersecurity Guide Delayed **

The federal government is pushing back plans to unveil the National Strategy to Secure Cyberspace, a roadmap for securing cyberspace, from this summer to mid-September. Richard Clarke, White House special adviser for cyberspace security, said the plan, which has been under way for several months, will not be written by bureaucrats, but by people in such areas as higher education, banking, transportation, and state and local governments.

Read more: http://www.hipaadvisory.com/news/index.cfm#0617fcw

** JCAHO Not HIPAA Enforcer **

Two common misconceptions concerning the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) were clarified at the Healthcare Information and Management Systems Society's (HIMSS) Summer Conference this week in Las Vegas. Speaking at the conference, Richard Croteau, M.D., executive director for strategic initiatives at JCAHO, said that JCAHO will not enforce HIPAA requirements, despite what some attorneys and consultants have been purporting in recent years. "We will survey compliance with accreditation standards, not HIPAA regulations." Another misconception, according to Croteau, is that HIPAA and JCAHO requirements conflict with each other. "There are no contradictions between HIPAA and JCAHO standards," contends Croteau.

** Spam, Viruses Hit Bottom Line Harder in US than in Europe **

Computerworld reports the intrusion of viruses and spam on corporate networks has grown from an annoyance to a costly problem in the U.S., even forcing companies to double up on prevention. In Europe, however, privacy protections may be limiting the spam problem. Aetna, Inc. runs Trend Micro's InterScan software along with Symantec antivirus software to scan incoming emails for viruses and spam. "Our belief is that most security products fail eventually, in some way. But when they do, they don't [all] fail in the same way," said Alan Pawlak, security manager at Aetna.

Read more: http://www.hipaadvisory.com/news/index.cfm#0617cw

** Genome Project will Challenge CIOs **

The human genome project will be an "incredible" information technology challenge, the biggest in the next generation, says Gregory Stock, M.D., director of the program on medicine, technology and society at UCLA School of Medicine. "There will be tension between privacy, safety and progress," Stock predicted at the HIMSS' Summer Conference this week, reports Health Data Management. "If you put a lock around the privacy of medical records, you will slow development of new technologies." Future advances in gene knowledge also will significantly affect the insurance industry and will generate a re-examination of patient privacy rights. If consumers have access to information on their predisposition toward specific diseases and that information is not available to insurers, consumers with a genetically higher risk of disease will load up on insurance. But if insurers get such information, large segments of the population may not be able to get or afford health coverage.

Read more: http://www.hipaadvisory.com/news/index.cfm#0614hdm3

** HIPAA May Forbid Sports Leagues to Say if Player Is Hurt **

According to the New York Times, HIPAA may prevent major sports league officials who talk about injuries from disclosing a player's medical information without consent. If professional and amateur players assert privacy rights as provided by the law, the resulting information embargo could affect betting lines, trades, bidding for free agents. Rob Manfred, the chief labor lawyer for Major League Baseball, said that while the law might be useful in other businesses, "it doesn't make sense that the New York Yankees can't tell their fans about the condition of their star pitcher."

Read more: http://www.hipaadvisory.com/news/index.cfm#0611nyt

==========

3 >> H I P A A / EDI: Q/A on Transactions & Code Sets

** The Newly Published HIPAA Rules -- How To Respond? **

by Kepa Zubeldia, M.D., President/CEO of Claredi

QUESTION 1): What transactions should my organization implement, the HIPAA transactions published in May 2000, or the new transactions in the recently proposed NPRMs?

ANSWER: It depends. The Addenda to the HIPAA transactions, in the proposed rules published May 31 (see them at http://www.hipaadvisory.com/regs/Regs_in_PDF/electrans.pdf) are changes and improvements to the original HIPAA transactions from May 2000. In most cases they are changes that were considered "necessary for implementation" by the transaction developers. In fact, the referral (278) transaction has very substantial changes in the proposed Addenda. Without these changes, the May 2000 version of the Referral is considered by many to not be implementable. Other transactions have fewer changes. Overall, except for the Referral transaction, the Addenda changes less than 5% of the transaction requirements.

If you choose to implement the Addenda, be aware that they could be subject to change, based on the comments during the NPRM comment period that closes on July 1st. However, since the Addenda were written by industry consensus, we would expect the changes in the Final Rule to be minimal, if any.

If you have observed how civil engineers build new highway intersections, you have a good model for building the HIPAA transactions. The trick is to go from where we are today to where we need to be in about 16 months without disrupting the heavy traffic through these electronic highways. Some times,

in the process of construction, the three-lane highway will have to be reduced to only one lane for a while. Other times, in order to build a new bridge, a temporary bridge must be built first, so the traffic can be diverted.

We should not confuse the temporary bridge, with flimsy guardrails and poor lighting, with the desired end result. And we should not be frustrated by the slowdown caused by the one-lane restriction. At the end of the construction project, the traffic will flow much better and it will be safer and more efficient for all. In this example, the Addenda could be compared to a new top coat of asphalt or a new paint job.

The May 2000 version has some problems. The Addenda version corrects some of these problems. Not all problems, just the biggest ones. There will be new versions. The industry needs are constantly changing. The traffic is increasing. We will learn to use new transactions. In the process there will be new potholes, diversions, slowdowns, accidents, etc. As the process matures, the transactions mature, we gain new experience, the friction will be reduced, the efficiency will increase, the cost will decrease.

The HIPAA transactions as we know them today will evolve. The pioneers that are ahead of the implementation curve are the ones that are falling into the sandtraps, getting stuck in the tar pits, and discovering the new territory for the rest of the industry. Those that follow will benefit from their experience. We need to apply their experience to our situations. How will I resolve the specific problem they have encountered? Will their solution work for me?

It is critical that the entire industry share ideas on how to solve these problems. Mailing lists like this one, collaborative groups like the regional SNIP groups, trade associations like AFEHCT, are helping all of us in sharing solutions to these problems. When a pioneer stumbles on a rock, instead of saying "their step faltered," we ought to just flag that obstacle as something for us to avoid. Learn from others' mistakes, instead of criticizing them for making mistakes.

Let me applaud the efforts of the HIPAA pioneers. They are solving very difficult problems. They are making our future easier. Instead of wondering what transactions to implement - the May 2000 or the Addenda - they are busy implementing them. I want to learn from their mistakes.

QUESTION 2): Does the new "Employer ID" Final Rule affect HIPAA transactions other than the 824 Enrollment transaction?

ANSWER: Because we don't have HIPAA Provider IDs or HIPAA Health Plan IDSs, the Final Rule on Employer ID potentially affects *all* of the HIPAA transactions, not just the 834 Enrollment transaction.

Until the Provider and Health Plan Identifiers are adopted under HIPAA, transactions such as the 837 (Claims) and the 835 (Remittance Advice) use other identifiers (submitter's choice) for Providers and Health Plans.

Lacking the HIPAA National Provider ID, the typical choice is either the EIN, the SSN, or some other pre-HIPAA ID. Since most providers will not want to use their SSN, most providers will be using the EIN as their primary Provider ID.

If you use the EIN as identifier in any of the HIPAA transactions, the Employer ID Final Rule needs to be taken into account.

In choosing the IRS-issued EIN as a HIPAA standard, the Final Rule specifies that the EIN must be used exactly as issued by the IRS. Currently, the EIN issued by the IRS is in the format 00-0000000, including the hyphen. The hyphen, according to the final rule, is an important part of the EIN under HIPAA.

However, most healthcare EDI today does not use the hyphen in the EIN, just the digits.

So, for HIPAA, the EDI transactions will need the hyphen to be transmitted as part of the data. This is something the EDI translation software can do automatically. Just make sure your programmers know about it.

Kepa Zubeldia, M.D., is President and CEO of Claredi, a leading provider of HIPAA EDI compliance testing and certification. http://www.claredi.com

==========

4 >> H I P A A / LAW : Legal Q/A

** Covered Entities as Employers -- How Does HIPAA Apply? **

by Steve Fox, Esq., & Rachel Wilson, Esq.

QUESTION: As a healthcare "covered entity," does my organization also have HIPAA responsibilities as an employer?

ANSWER: If your organization is like most health care providers, health plans, and health care clearinghouses subject to HIPAA's administrative simplification provisions ("Covered Entities"), it is very aware of its obligations to maintain the privacy and security of certain patient health information. Toward that end, you and your colleagues are likely in the process of implementing the safeguards, procedures, and policies necessary

to provide patients with at least a minimum standard of privacy protection. All of which is great - but you cannot forget to include protections for the health information of your employees. HIPAA is applicable to you in your role as employer as well as Covered Entity.

Employers are not Covered Entities subject to direct regulation under HIPAA. However, in their role as group health plan sponsors, employers generally have certain compliance obligations under HIPAA's privacy rule (the "Privacy Rule") as business associates. These obligations arise out of the functions performed by the plan sponsor in connection with the administration of benefits.

Any protected health information ("PHI") that is used or disclosed to perform such functions is protected under HIPAA, as are the corresponding activities carried out by the plan sponsor's workforce. Accordingly, health plans may not release PHI to plan sponsors unless and until such sponsors certify that the plan documents have been amended to incorporate provisions that:

* establish the permitted uses and disclosures of PHI,
* prohibit the use or disclosure of PHI except as permitted or required by the plan documents or as required by law;
* ensure that any agents, to whom the plan sponsor provides PHI, are bound by the same restrictions and conditions that apply to the plan sponsor with respect to such information;
* prohibit the plan sponsor from using or disclosing PHI for employment-related actions and decisions or in connection with any other benefit or benefit plan;
* require the plan sponsor to report any use or disclosure of the PHI that is inconsistent with the permitted uses and disclosures;
* make certain that PHI will be made available to individuals in accordance with the applicable terms of the Privacy Rule; and
* ensure separation between the plan sponsor and the plan.

This latter item is to be accomplished by restricting the use and disclosure of PHI, limiting access to PHI, and developing a mechanism to resolve issues of noncompliance with such use, disclosure, and access restrictions.

The proposed security rule under HIPAA (the "Security Rule") will also likely have application to Covered Entities in their role as employers. Although plan sponsors are not Covered Entities, they may, nevertheless be required to comply with the Security Rule by executing chain of trust agreements to insure the security of data transmitted electronically between the sponsor and Covered Entity.

Read past HIPAA Legal Q/A articles:

http://www.hipaadvisory.com/action/LegalQA/archives.htm

Steve Fox, Esq., is a partner at the Washington, DC office of Pepper Hamilton LLP. This article was co-authored by Rachel H. Wilson, Esq., of Pepper Hamilton LLP. http://www.pepperlaw.com/
Disclaimer: This information is general in nature and should not be relied upon as legal advice.

==========

5 >> H I P A A / SECURE: Security Q/A

** Re-Thinking Computer Disposal Under HIPAA **

by Eric Maiwald, CISSP

QUESTION: What should we do about information that may be on computers that we are getting rid of?

ANSWER: This is a very timely question. Many organizations get rid of computers by donating them to schools or non-profit organizations. Others work out a deal with their vendors to take the old computers as new ones are put in place. In either case, there may be sensitive information on the disks in those systems.

Before we go too much further, let's talk a little about how information is actually stored on the disk. A hard disk is magnetic media. In other words, information is stored on the disk by changing the magnetic characteristics of a certain spot on the disk. As files are written to the disk, the location of the file is also written to another section of the disk. If a file is deleted, the only information that is erased is the information about the location of the file. The information in the file itself remains on the disk. The same is true if a disk is formatted. In this case all of the information about where files are located is erased but the information on the disk remains.

There are a number of tools that can read information on disks even if the disk has been formatted. Therefore, the only way to truly remove information from the disk is to overwrite the specific parts of the disk that contain the information. While you could do this manually, it is much more efficient to do this with a disk wiping tool such as Cyberscrub (http://www.cyberscrub.com - they also have a product called Cybercide intended for use on computers that are being recycled or returned to a vendor). Tools like this overwrite the entire disk or just the location of a specific file multiple times to make sure that the information is unreadable.

One thing to keep in mind when looking for a tool like this is to find one that uses the Defense Department Standard (DoD 5220.22). This standard requires that the disk be overwritten in several ways - first with zeros, then with ones, then with random numbers between 2 and 9. This makes it much more difficult for anyone to get at the information.

Performing this type of action on every old computer may seem like a lot of work. However, think about the sensitive information that may be on those computers. It could be patient information, salary information, or just the personal information about an employee. When you consider the risks, it is well worth the time and effort to clean the systems.

Eric Maiwald, CISSP, is Chief Technology Officer of Fortrex Technologies, which provides information security management, process and monitoring services for healthcare organizations and other industries.
http://www.fortrex.com

==========

6. H I P A A v i e w:

** HIPAA Costs -- Are Small Hospitals Taking Too Big a Hit? **

by Roy Rada. M.D., Ph.D.

Surveys of HIPAA compliance progress provide valuable information about the industry's common practices. Mining of the data results of one of the more influential surveys, the "U.S. Healthcare Industry Quarterly HIPAA Compliance Survey Results," run quarterly by Phoenix Health Systems, raises interesting questions. One provocative question is whether small hospitals are paying disproportionately more to achieve HIPAA compliance than large hospitals.

The Data

All the data presented here come from the "Winter 2001-2002" survey that is publicly available at
http://www.hipaadvisory.com/action/surveynew/Winter2002.htm. (The recently-published Spring 2002 Survey reports spending remains substantially the same.) As one looks at the data about how much small, medium, and big hospitals are reportedly spending on HIPAA compliance, the obvious first conclusion is that bigger hospitals spend more than smaller hospitals. In the survey,

* small hospitals are those with fewer than 100 beds,

* medium sized hospitals are between 100 and 400 beds in size, and
* large hospitals have more than 400 beds.

In predicted expenditures for 2002, all of the small hospitals are spending less than $300K and over half of the large hospitals are spending more than $300K. One would expect this. The bigger question is "Will economies of scale prevail?" In other words, do bigger hospitals spend less per bed?

By taking the small and medium-sized hospitals, we can estimate their average bed size as 50 beds and 250 beds, respectively. (Estimating the size of hospitals with more than 400 beds is difficult without knowing more about the respondents). By taking the mid-point of the budgeted HIPAA expenditures for 2002, we can guess that a hospital planning to spend between $100K and $300K will spend $200K and so on. From these assumptions, let's infer that medium-sized hospitals are spending about $800 per bed and small hospitals are spending about $1,600 per bed.

Different Strokes for Different Folks

The Privacy Rule emphasizes scalability, i.e., flexibility. Small entities are not expected to have as complex an approach as large entities. For instance, a small physician practice could essentially ignore the Minimum Necessary Standard - everyone may need to see everything. However, within the large entity, the Minimum Necessary Standard may entail a delineation of what the roles of the entity are, what the categories of protected health information are, and what roles should access what categories of information. Such flexibility would imply that a small entity need not have high compliance costs.

As the survey shows that the costs of small entities per bed are double those of medium sized entities, one wonders why. There are two possibilities:

* "Economies of scale" doom the smaller entity to a higher per capita cost or
* Smaller entities are taking too rigorous an approach.

In either case, the smaller entities should rely on their peer entities for help. By working together to share information and agree on a common approach to compliance, entities can reduce their costs. For small entities, this means communicating through various means with their peers about the tools for compliance and agreeing that simple tools will do the job. The government would be hard pressed to prosecute an entity that could demonstrate that it was using practices agreed upon by peers.

Transactions versus Privacy

The data offers other stories. The survey data reports the percent of respondents involved in each phase of the compliance life cycle for privacy and for transactions. One might expect different patterns for privacy than for transactions based on entity size. Smallish entities might rely on a clearinghouse for transactions compliance, while larger entities may be moving into advanced stages of transactions compliance activity as they overhaul their systems to take advantage of standard transactions. One can look at the life cycle of compliance data and compare the number of respondents of a given entity size in advanced stages of privacy activity with those in advanced stages of transactions activity. The result is that smaller entities are relatively advanced in their privacy efforts relative to their transactions efforts. Large entities are about equally advanced in the privacy and transactions phases of compliance.

Roy Rada, M.D., Ph.D., is Professor, Health Care Information Systems, University of Maryland, Baltimore County, and a frequent industry speaker on HIPAA-related issues.

==========

Join us June 26, 2 PM EST for our next HIPAA audioconference...

** HANDS-ON HIPAA:
A Professional Approach to Costing Your HIPAA
Remediation Project **

This not-to-be-missed program presents a detailed, professional approach to budgeting your organization's HIPAA remediation project.

SIGN UP TODAY! http://www.hipaadvisory.com/ezcart/

==========

BRING YOUR HIPAA QUESTIONS AND IDEAS TO LIFE AT...
H I P A A l i v e !

Join nearly 5,000 other thinkers, planners, learners and lurkers who are already members of our sister email discussion list. We almost make HIPAA fun! Almost. (Also available in a PREMIUM version of easy-to-navigate, individually formatted, "cleaned up" digests.) Subscribe now at:
http://www.hipaadvisory.com/live/
==========

RAISE YOUR ORGANIZATION'S HIPAAWARENESS WITH
H I P A A n o t e s !

Over 10,000 subscribers already receive our weekly byte of HIPAA. HIPAAnotes are suitable for publishing on your organization's intranet or newsletter & come free to your emailbox. Subscribe now at:
http://www.hipaadvisory.com/notes/

==========
You are currently subscribed to hipaalert
as: kmckinst@dmhhq.state.ca.us
======
To view the list's archives, change your settings (e.g., your email address, switch to HTML or text version, set to 'nomail' while you're away), or UNSUBSCRIBE, go to:
http://lyris.dundee.net/cgi-bin/lyris.pl?enter=hipaalert